Job Aid: Incident and Reportable Event Categories

Source: CJCSM 6510.01A Enclosure B, Appendix A, Incident and Reportable Event Categorization

	Precedence	Category	
INCIDENTS	1	1	**Root Level Intrusion (Incident)** Unauthorized privileged access to a DOD system. Privileged access, often referred to as administrative or root access, provides unrestricted access to the system. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
	2	2	**User Level Intrusion (Incident)** Unauthorized non-privileged access to a DOD system. Non-privileged access, often referred to as user-level access, provides restricted access to the system based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the system is compromised with malicious code that provides remote interactive control, it will be reported in this category.
	3	4	**Denial of Service (Incident)** Activity that denies, degrades, or disrupts normal functionality of a system or network.
	4	7	**Malicious Logic (Incident)** Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This **only** includes malicious code that does not provide remote interactive control of the compromised system. Malicious code that has allowed interactive access should be categorized as Category 1 or Category 2 incidents, not Category 7. Interactive active access may include automated tools that establish an open channel of communications to and/or from a DOD system.

	Precedence	Category	
EVENTS	5	3	**Unsuccessful Activity Attempt (Event)** Deliberate attempts to gain unauthorized access to a DOD system that are defeated by normal defensive mechanisms. Attacker fails to gain access to the DOD system (i.e., attacker attempt valid or potentially valid username and password combinations) and the activity cannot be characterized as exploratory scanning. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
	6	5	**Non-Compliance Activity (Event)** Activity that potentially exposes DOD systems to increased risk as a result of the action or inaction of authorized users. This includes administrative and user actions such as failure to apply security patches, connections across security domains, installation of vulnerable applications, and other breaches of existing DOD policy. Reporting of these events is critical for the gathering of useful effects-based metrics for commanders.
	7	6	**Reconnaissance (Event)** Activity that seeks to gather information used to characterize DOD systems, applications, networks, and users that may be useful in formulating an attack. This includes activity such as mapping DOD networks, systems devices and applications, interconnectivity, and their users or reporting structure. This activity does not directly result in a compromise.
	8	8	**Investigating (Event)** Events that are potentially malicious or anomalous activity deemed suspicious and warrant, or are undergoing, further review. No event will be closed out as a Category 8. Category 8 will be re-categorized to appropriate Category 1-7 or 9 prior to closure.
	9	9	**Explained Anomaly (Event)** Suspicious events that after further investigation are determined to be non-malicious activity and do not fit the criteria for any other categories. This includes events such as system malfunctions and false alarms. When reporting these events, the reason for which it cannot be otherwise categorized must be clearly specified.